AU/ACSC/YAMAGUCHI/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Development of JSDF Cyber Warfare Defense Critical Capability

by

Yoshihiro Yamaguchi, Major, Japan Air Self Defense Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Black, Mark L and Griffith, Paul E

March 2010

Abstract

Notwithstanding potential adversaries may try to attack national vital infrastructures thorough internet as a means of warfare, it is extremely difficult to distinguish an offensive cyber attack as a military activity from cyber criminals or cyber vandals. Despite of these difficulties, "cyber-attack identification capability" is essential for a nation to defend her vital infrastructures against offensive cyber warfare. Although the necessity of cyber-attack identification capability is quite clear, the Japan's preparation against cyber warfare is quite limited.

In this paper, the author illustrates the problems related to Japan's preparation for defensive cyber warfare. Then, the author makes some recommendations to develop cyber identification capability in Japan Self Defense Force (JSDF). It will include technology, the appointment of JSDF as a main player to defend military cyber attack, establishment of cyberspace defense operation center, enhancement of personal capabilities of SDF C4 System Command, and conduct of cyber defense exercise with other organizations.

Now, we are in a new era called "the information age." Modern societies heavily rely on information communication technology (ICT) to maintain many kinds of national vital infrastructures, such as electric grid, oil, gas and water supply, transportation, and financial market. Of course, Japan is not an exceptional, rather one of the most ICT dependent countries. Although ICT promote convenience and efficiency, it also produces the critical vulnerabilities of national instrument of power. Notwithstanding potential adversaries may try to attack national vital infrastructures thorough internet as a means of warfare, it is extremely difficult to distinguish an offensive cyber attack as a military activity from cyber criminals or cyber vandals.

Despite of these difficulties, "cyber-attack identification capability" is essential for a nation to defend her vital infrastructures against offensive cyber warfare, because a nation cannot respond "Cyber Pearl Harbor" effectively without identifying military activities or not. In this short essay, the author demonstrates the necessity of cyber-attack identification capability to defend Japanese vital infrastructure against offensive cyber warfare, the current situations and problems of Japanese cyber-warfare preparations. Then, I try to make recommendations to develop cyber identification capability in Japan Self Defense Force (JSDF).

The identification capability of cyber warfare is vital to defend Japanese national interests. After WWII, Japan recovered from disastrous situation and succeeded in developing as an economic developed nation. In 1990s, governmental organizations and many civilian companies began to take advantage of usefulness of ICT capabilities together with the development of ICT. In 2000, Japanese government chose "E-Japan Strategy" as a means to achieve as the world highest ICT developed country. The number of population who use the broadband internet access technology such as ADSL and FTTH grew rapidly and reached over ninety million in 2009.[1] In

response to the rapid growth of ICT in Japan, the total number of internet crime has been increasing continuously.

In those situations, potential adversaries may launch cyber attacks against Japan's vital infrastructures as a means of military activities. They may simultaneously attack computer systems that support not only JSDF command systems, but also electric power grid, city gas distribution system, railway control system, air traffic control system, and Tokyo stock exchange. If they succeeded in such kinds of simultaneous cyber attacks at the beginning of surprise military aggression, the results might be disastrous because it would be difficult to identify the attack as a military aggression immediately.

In order to effectively respond such kinds of offensive cyber warfare, cyber-attack identification capability is vital for JSDF. JSDF can only take self defense actions to mitigate the damage of these cyber attacks without identifying cyber attacks as a means of warfare. The Armed Attack Situation Response Law determines the fundamental nature of Japan's response to armed attack situations and defines basic principles, and the responsibilities of national and local government in the event of an armed attack situation. According to the law, the government must justify the recognition of armed attack situation or situation where an armed attack is anticipated, and the fact that constituted the base of the recognition.[2] To justify JSDF's military response, it is essential to prove the attribution of cyber attack as an "armed attack." Therefore, JSDF should develop the identification capability of cyber warfare.

In spite of the necessity of cyber-attack identification capability, the current Japan's preparation against cyber warfare is quite limited. First, the defense responsibility of information systems which support national vital infrastructures depends on each organization. The major telecommunication companies establish network operation centers to control and surveillance

own network. The internet service providers also organize security operation centers to detect and protect cyber attacks and computer virus against their vital servers. Although these ICT companies have well-trained operation centers, other national vital service organizations and companies normally does not organize such kind of functions. For example, a civilian electric power company may only have a control center which manages electric power distribution, but there is no organization and function to detect cyber attacks.

Second, although the relationship among cyber attack response organizations has been becoming more capable than before, these organizations has no responsibility to identify cyber warfare. Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is one of the core organizations which have highly capabilities to respond cyber incidents. The activities of JPCERT/CC include incident response and analysis, security alert, coordination with other CSIRTs, vendor coordination, education and training, and research and analysis. JPCERT/CC collaborates with major ICT companies' network and security operation centers and establishes Internet Scan Data Acquisition System (ISDAS), which has a wide distributed arrangement of sensors, and observes various scan activities; worm infections, probing vulnerable systems.[3] Although JPCERT/CC has capabilities and connections with other companies, it is not a governmental organization but an independent administrative institution and has no responsibility to react cyber warfare.

Third, the governmental authority of information system protection over civilian companies is quite weak. The government legislates many kinds of security standards such Information Security Management System (ISMS), and Integrated Standards of Information Security Protection. However, there are no comprehensive laws that regulate the security level a company must fulfill.

Finally, the JSDF's cyber warfare capabilities are quite limited. In 2008, the Ministry of Defense established the SDF C4 System Command which directly reporting to the Chief of Staff of the Joint Staff Office. Moreover, all three services of JSDF have system protect units or squadrons. However, the mission of these units focuses on the protection of military computer network systems. These units have no responsibility and capability to protect the information systems that support national vital infrastructures outside of the JSDF.

In sum up, although the necessity of cyber-attack identification capability is quite clear, the Japan's preparation against cyber warfare is quite limited. Moreover, the Ministry of Defense and JSDF has not developed the consensus to establish the comprehensive capability of the strategic cyber warfare defense, covering systems of the national vital infrastructures as well as military command systems.

However, can we do identify a cyber attack as a "military activity?" It is true that identifying the attribution of cyber attack is quite difficult. In order to avoid being identified by cyber police, almost all hackers personate or hijack other person's computer and utilize as a vicarious intruder. Distributed denial-of-service (DDoS) attack, one of the most popular and easiest ways to neutralize targeted server, is also launched by trapped computers. The owners of these hijacked computers are unaware that they are attacking targeted server. Therefore, although cyber police can attribute the source of DDoS attack to these hijacked computers, it is difficult to determine "real attacker" of DDoS attack.

However, in order to establish defensive cyber warfare capabilities in JSDF, identification technology of cyber attacks is vital. If JSDF cannot obtain identification technology of cyber attacks, it will be impossible to conduct defensive action against strategic

cyber offensive operation. Therefore, this technology will be a key to conduct cyber warfare both offensive side and defensive side.

Although it is quite difficult to identify the source of cyber attack today, it is not impossible to do that in the near future. “IP traceback” is one of the key technologies. When a traceback system is introduced on the Internet, ISP operators will be able to confirm the passage of specified packets among ISPs (ASs), and be able to track the attacker’s ISP when the security incident occurs, and identify the bottleneck ISP when the network becomes congested.[4]Large scale demonstration experiment was conducted in Japan from April to September in 2009. Fifteen major ISPs and three research centers participated in the experiment. Using real internet, they succeeded in tracing the source of cyber attack that was personated to different IP address and passed through fifteen different ISPs. This was the first successful experiment in the world to trace back the source of attack through different ISPs in the real internet. Although there are some technical and legal challenges, it will be possible to identify the source of cyber attack near future. This technology is very similar with the birth of Radar in 1935. Detecting intrusion air plane was impossible in early 1930s. However, the Great Britain succeeded in developing/utilizing Radar technology and integrating command center and fighter wings to defend the nation. “IP traceback” may be “Radar of cyberspace” in near future.

The first step of JSDF to establish cyber-attack identification function is the appointment of JSDF as main player to cyber warfare defense of Japan. As mentioned before, there is no consensus to invest JSDF with cyber warfare defense responsibility by not only Japanese government but also the Ministry of Defense. Japan is surrounded by potential threats of cyber warfare such as China, Korea and Russia. Especially, historical arguments among Japan, China and Korea agitate intolerant nationalism and lead conflict in cyber space. There is no proof that

these cyber attacks are related to activities of military organizations. However, these nation states may utilize nationalism as a means of information warfare and indirect military attacks. Therefore, Japanese government must recognize these potential threats as military threats and invest JSDF with cyber warfare defense responsibility.

The second step is to create the cyber space defense operation center inside the SDF C4 System Command. This operation center must integrate situational awareness of cyber space not only SDF's closed network and command systems, but also civilian major telecommunication networks, major ISPs and information systems of critical infrastructures. However, it will be impossible to create sensor network which is only for military purpose, in terms of limited JSDF's budgets. Therefore, JSDF should obtain situational awareness of cyberspace from other organizations. Governmental and Non-governmental organizations, such as National Information Security Center (NISC), JPCERT/CC, @police (the cyber force of the National police Agency in Japan), network and security operation centers of major ICT companies, and security software vendors, have already created their own sensor networks in internet. Particularly, NISC and JPCERT/CC play the major roles to integrate information from these organizations. SDF C4 System Command needs to establish connections among these key organizations in order to obtain situational awareness.

The third step is to enhance the capability of defensive cyber warfare of SDF C4 System Command. Ministry of Defense decided to establish "Cyber space defense unit" under SDF C4 System Command in 2011. Because of limited number of personnel, all members of the unit must focus on staying up to date as new technologies. Maintaining and enhancing ICT capabilities is critical to conduct defensive cyber warfare. Greg Rattray, the author of "Strategic Warfare in Cyberspace", also pointed out that "Defensive strategic information efforts, like those

involved in offensive strategic information warfare, require pool of human capital with advanced technological skills."[5] Although all services established technical schools related to information technologies, it is difficult for these schools to catch up with development of new technologies. Therefore, members of the unit should be temporary transferred to ICT companies, JPCERT/CC and security software vendors to learn the latest technology of cyberspace. This program will be effective not only to enhance member's capability but also to promote personal relationship with civilian expertise. Moreover, some of the unit members must enhance not only cyber capabilities but also knowledge and experiences about the reality of military operations. Excessively "IT focused" personnel may lose sight of the relationship between cyber attack and conventional military attack.

The forth step is to conduct comprehensive cyber defense exercises. In terms of defensive cyber warfare, Ministry of Defense must be in charge of these exercises. Now, although we have no "cyber warfare" training with civilian companies, Ministry of Internal Affairs and Communications (MIC) has conducted "cyber attack response exercise in telecommunication fields"[6] since 2007. The Prime Minister and His Cabinet and three major ICT companies – NTT, KDDI and IIJ- participated in the exercise. The purpose of exercise was to synergistically respond against supposed DDOS attack. However, MOD and JSDF did not participate in the exercise because MIC focused on only "cyber crime" against Japan and had no standpoint of "cyber warfare." Therefore, MOD should take initiative to conduct comprehensive cyber warfare defense exercises in the future. Identification of military cyber attack will be the most important role of SDF C4 System Command. For these reasons, in the exercises, SDF C4 System Command should focus on identifying whether the attack is "military cyber attack" or not. If SDFC4 System Command successfully identifies the attack as a military cyber attack, they must

justify their defensive reaction with proof. In order to identify and obtain evidences of military cyber attack, it is obvious that synergistic response among MOD and other organization will be vital. The cyber warfare defense exercise will be essential to enhance not only JSDF capability but also the relationship among related organizations.

In conclusion, Japanese government, especially MOD, must recognize the necessity of preparing strategic cyber warfare defense and establish defensive cyber warfare capabilities in JSDF. In order to conduct comprehensive reaction against military cyber attack, identification capability will be a vital technology. Moreover, collaboration with JSDF and other organizations outside of MOD is essential to identify a cyber attack as a military operation. There will be four steps to prepare defensive cyber warfare; the appointment of JSDF as a main player to defend military cyber attack, establishment of cyberspace defense operation center, enhancement of personal capabilities of SDF C4 System Command, and conduct of cyber defense exercise with other organizations. These preparations will be vital to prepare future cyber warfare against Japan.

Bibliography

Gregory J. Rattray, *"Strategic Warfare in Syberspace"*, (The MIT press Cambridge, Massachusetts London, England, 2001)

JPCERT/CC, "What is ISDAS?" <http://www.jpcert.or.jp/english/isdas/readme.html>

Ministry of Internal Affairs and Communications in Japan, "Communications Usage Trend Survey in 2009" <http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html>

Ministry of Internal Affairs and Communications, *Cyber attack response exercise in telecommunication fields*, (Ministry of Internal Affairs and Communications, Tokyo, Japan, 2009)

Ministry of Defense, *Defense of Japan 2009 –Japanese defense white paper in 2009* (Tokyo, Japan)

Ken Wakasa et al., *Demonstration Experiments Towards Practical IP Traceback on the Internet,* (Japan Data Communications Association, Tokyo, Japan, 2009)

[1] Ministry of Internal Affairs and Communications in Japan, "Communications Usage Trend Survey in 2009" http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html (accessed 31 January 2010).
[2] Ministry of Defense, *Defense of Japan 2009 –Japanese defense white paper in 2009* (Tokyo, Japan), 173, 428.
[3] JPCERT/CC, "What is ISDAS?" http://www.jpcert.or.jp/english/isdas/readme.html (accessed 31 January 2010).
[4] Ken Wakasa et al., *Demonstration Experiments Towards Practical IP Traceback on the Internet,* (Japan Data Communications Association, Tokyo, Japan, 2009) https://www.telecom-isac.jp/tb/index_e.html (accessed 2 March 2010)
[5] Gregory J. Rattray, "*Strategic Warfare in Syberspace*", (The MIT press Cambridge, Massachusetts London, England, 2001), 222.
[6] Ministry of Internal Affairs and Communications, *Cyber attack response exercise in telecommunication fields*, (Ministry of Internal Affairs and Communications, Tokyo, Japan, 2009) http://www.soumu.go.jp/menu_kyotsuu/media/080401_1.html (accessed 3 March 2010)